IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

In re Onix Group, LLC Data Breach Litigation	Civil Action No. 23-2288-KSM **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Eric Meyers, Donald Owens, Aida Albino Wimbush, Ashtyn Mark, Leah Simione, Melissa Lyston, and Angela Haynie ("Plaintiffs") bring this Consolidated Class Action Complaint against the Onix Group, LLC ("Onix" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and good faith belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Onix for its failure to properly secure and to safeguard the personally identifiable information of hundreds of thousands of people.

2. Onix is a conglomerate that operates in the hospitality, commercial real estate development and healthcare industries.[1] The data breach at issue in this case impacted the following groups: Addiction Recovery Systems, Cadia Healthcare, Physician's Mobile X-Ray, Onix Group, and Onix Hospitality Group.[2]

[1] https://www.onixgroup.com/about-onix/ (last visited Sept. 13, 2023).

[2] Sample Onix *Individual Notification Letter*, available at https://www.onixgroup.com/wp-content/uploads/2023/05/Onix-Notice-of-Data-Security-Incident.pdf (last accessed Sept. 13, 2023).

3. On March 27, 2023, Onix experienced a targeted ransomware attack that affected its internal computer systems and allowed an unauthorized third party to exfiltrate extremely sensitive and personally identifying information including, but not limited to: names, Social Security numbers, dates of birth and clinical information (collectively, the "Private Information" or "PII and PHI") stored thereon (the "Data Breach").[3] Onix subsequently confirmed that an unauthorized actor accessed its systems between March 20, 2023 and March 27, 2023 and removed a subset of files, including, but not limited to, the Private Information of Plaintiffs and Class Members.

4. On or around May 26, 2023, Onix sent a Notice of Data Breach (the "Notice Letter") informing Plaintiffs and Class Members of the following:

> **What happened?** [Onix] experienced a ransomware incident on March 27, 2023, that affected [Onix's] internal computer systems. [Onix] took immediate action to secure [Onix's] systems and launched an investigation with help from cybersecurity experts. The investigation determined that an unauthorized person accessed [Onix's] network between March 20, 2023 and March 27, 2023, corrupted certain systems, and removed a subset of files. [Onix's] electronic medical records application was not impacted.
>
> **What Information Was Involved?** The information contained in the files varied by individual, but may have included your name, Social Security number, date of birth, and clinical information regarding [Plaintiffs'] care...

5. Onix, in its Notice Letter, acknowledges that Plaintiffs' and Class Members' Private Information was unlawfully accessed and exfiltrated.

6. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Onix's inadequate safeguarding of Class Members' Private Information that it collected

[3] https://www.onixgroup.com/wp-content/uploads/2023/05/Onix-Notice-of-Data-Security-Incident.pdf (last visited: Sept. 13, 2023).

and maintained, and for failing to provide adequate notice to Plaintiffs and Class Members.

PARTIES

7. Plaintiff Eric Meyers at all relevant times was and is a resident and citizen of Delaware.

8. Plaintiff Donald Owens at all relevant times was and is a resident and citizen of Virginia.

9. Plaintiff Aida Albino Wimbush at all relevant times was and is a resident and citizen of New Jersey.

10. Plaintiff Ashtyn Mark at all relevant times was a resident and is a citizen of Pennsylvania.

11. Plaintiff Leah Simione at all relevant times was and is a resident and citizen of New Jersey.

12. Plaintiff Melissa Lyston at all relevant times was and is a resident and citizen of New Jersey.

13. Plaintiff Angela Haynie at all relevant times was and is a resident and citizen of Delaware.

14. Defendant Onix Group, LLC is a Foreign Limited Liability company (formed in Delaware) with its principal place of business located at 150 Onix Drive, 2nd Floor in Kennett Square, Pennsylvania 19348.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

17. This Court has subject matter jurisdiction over this action further to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because: (i) the amount in controversy exceeds $5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiffs Meyers, Owens, Wimbush, Simione, Lyston, Mark, and Haynie, have different citizenship from Defendant.

18. This Court has personal jurisdiction over Defendant because it operates and is headquartered in this District and conducts substantial business in this District.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiffs' and Class Members' Private Information in this District, and has caused harm to Plaintiffs and Class Members in this District.

FACTUAL ALLEGATIONS

Defendant's Business

20. As a condition of providing services, Onix requires that patients of the entities it operates entrust it with their Private Information.

21. Onix collects and maintains the Private Information of patients of its healthcare network, including but not limited to their:

- name,
- address,
- phone number and email address;
- date of birth;
- demographic information;

- Social Security number;
- financial information;
- information relating to individual medical history;
- information concerning an individual's doctor, nurse, or other medical providers;
- medication information;
- health insurance information;
- photo identification; and;
- other information that Onix may deem necessary to provide its services.

22. Additionally, Onix may receive Private Information from other individuals and/or organizations that are part of a patient's "circle of care," such as referring physicians, customers' other doctors, customers' health plan(s), close friends, and/or family members.

23. Because of the highly sensitive and personal nature of the information Onix acquires and stores with respect to its healthcare entities' patients and other individuals, Plaintiffs and Class Members reasonably expect that Onix will, among other things: keep their Private Information confidential; comply with healthcare industry standards related to data security and Private Information; inform them of legal duties and comply with all federal and state laws protecting their Private Information; only use and release their Private Information for reasons that relate to medical care and treatment; and provide adequate notice to them if their Private Information is disclosed without authorization.

24. Plaintiffs and Class Members entrusted Onix with their Private Information but, contrary to Onix's duties, promises, and the reasonable expectations of Plaintiffs and Class Members, Onix implemented substandard data security practices and failed to adhere to industry standard practices. Not only did Onix maintain inadequate security to protect its systems from infiltration by cybercriminals but it waited nearly two months to publicly disclose the Data Breach.

The Data Breach

25. According to the Notice Letter provided by Onix to Plaintiffs and Class Members,

Onix was subject to a cybersecurity attack culminating in ransomware from March 20-27, 2023.

26. On or about March 27, Onix discovered that the Data Breach may have impacted Private Information stored on its network.

27. In response, Onix stated that "we took immediate action to secure systems and launched an investigation with help from cybersecurity experts."[4]

28. As a HIPAA covered entity that collects, creates, and maintains significant volumes of Private Information, the targeted attack was a foreseeable risk of which Onix was aware and knew it had a duty to guard against.

29. This is particularly true because the targeted attack was a ransomware attack. It is well-known that healthcare businesses such as Onix, that collect and store the confidential and private information, including protected health information, of hundreds of thousands of individuals, are frequently targeted by ransomware attacks. Further, ransomware attacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper employee cybersecurity training. In fact, the vast majority of ransomware incidents are caused by a combination of poor user practices, lack of cybersecurity training, and weak passwords or access management.[5]

30. The targeted attack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of patients, including Plaintiffs and Class Members.

---

[4] https://www.onixgroup.com/wp-content/uploads/2023/05/Onix-Notice-of-Data-Security-Incident.pdf (last visited Sept. 13, 2023).

[5] "Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020." Statista, available at https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/ (last accessed Sept. 13, 2023).

31. Despite learning that the Data Breach compromised Private Information on March 27, 2023, Onix waited over two months following the completion of its investigation to notify the impacted individuals of the Data Breach and the need for them to protect themselves against fraud and identity theft. Onix was, of course, too late in the discovery and notification of the Data Breach.

32. Due to Onix's inadequate security measures and its delayed notice to victims, Plaintiffs and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

33. Onix had obligations created by the FTC Act, HIPAA, contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiffs and Class Members entrusted their Private Information to Onix with the reasonable expectation that Onix would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Onix's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the healthcare industry preceding the date of the breach.

36. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their personal information. Plaintiffs and Class Members would not have allowed Onix or anyone in Onix's position to receive their Private Information had they known that Onix would fail to implement industry standard protections for that sensitive information.

37. As a result of Onix's negligent and wrongful conduct, Plaintiffs' and Class Members' highly confidential and sensitive Private Information was left exposed to

cybercriminals. The unencrypted Private Information of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can now easily access the Private Information of Plaintiffs and Class Members.

Ransomware Attacks Are Preventable

38. Onix did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

39. Onix could have prevented this Data Breach by, among other things, properly encrypting Private Information or otherwise ensuring that such Private Information was protected while in transit or accessible.

40. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

41. To prevent and detect ransomware attacks like the one that led to the Data Breach, Onix could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, customers and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching

[6] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Sept. 13, 2023).

the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

42. To prevent and detect ransomware attacks like the one that led to the Data Breach, Onix also could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

[7] *Id.* at 3-4.

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[8]

43. Given that Defendant was storing and sharing the Private Information of its current and former patients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

44. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures, resulting in the Data Breach and the exposure of the Private Information of hundreds of thousands of Defendant's current and former patients' Private Information, including that of Plaintiffs and Class Members.

Defendant Knew or Should Have Known of the Risk Because Healthcare Entities In Possession of Private Information Are Particularly Suspectable to Cyberattacks

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the breach.

46. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

47. In 2021, a record 1,862 data breaches occurred, resulting in approximately

[8] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Sept. 13, 2023).

293,927,708 sensitive records being exposed, a 68% increase from 2020.[9]

48. Healthcare related breaches, in particular, have continued to rapidly increase because electronic patient data is seen as a valuable asset. In fact, entities that store patient information "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers."[10]

49. Moreover, in light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

50. Indeed, ransomware attacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[11]

---

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[10] Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, *available at*: https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks (last visited on Sept. 13, 2023).

[11] *See* https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-

51. A ransomware attack, like that experienced by Defendant, is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.[12] In a ransomware attack the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[13]

52. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[14] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

53. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[15] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[16] Once the data is exfiltrated from a network, its confidential nature is

---

aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last accessed Sept. 13, 2023).

[12] *Ransomware warning: Now attacks are stealing data as well as encrypting it*, available at https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/ (last accessed Sept. 13, 2023).

[13] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last accessed Sept. 13, 2023).

[14] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

[15] *2020 Ransomware Marketplace Report, available at* https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

[16] *Ransomware FAQs*, available at https://www.cisa.gov/stopransomware/ransomware-faqs

destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[17] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[18]

54. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

55. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

56. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

57. Additionally, as companies became more dependent on computer systems to run their business,[19] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of

---

[17] *Id.*

[18] *Id.*

[19] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html (last accessed Sept. 13, 2023).

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[20]

58. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially hundreds of thousands individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

59. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

60. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

61. As a healthcare services company in possession of current and former patients' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Onix Fails to Comply with FTC Guidelines

62. Onix is prohibited by the Federal Trade Commission Act (the "FTC Act") (15

[20] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022 (last accessed Sept. 13, 2023).

U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

63. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[21] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. *Id.*

65. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented

[21] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016).

reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. These FTC enforcement actions include actions against healthcare providers and partners like Onix. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

68. Onix failed to properly implement basic data security practices.

69. Onix's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. Onix was at all times fully aware of the obligation to protect the Private Information of its patients. Onix was also aware of the significant repercussions that would result from its failure to do so.

Onix Failed to Comply with HIPAA Guidelines

71. Defendant is a covered entity under HIPAA and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule

("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

72. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[22] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

73. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

74. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

75. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

76. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

77. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

[22] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

d. Ensure compliance by its workforce.

78. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

79. Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

80. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

81. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[23]

82. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

[23] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added). (last accessed Sept. 13, 2023).

83. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

84. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318.

85. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[24]

86. The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[25]

Onix Failed to Comply with Industry Standards

87. As shown above, experts studying cyber security routinely identify healthcare providers as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

---

[24] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Sept. 13, 2023).

[25] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Sept. 13, 2023).

88. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Onix, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

89. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

90. Onix failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

91. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Onix failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Onix Breached Its Duty to Safeguard Plaintiffs' and the Class's Private Information

92. In addition to its obligations under federal and state laws, Onix owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being

compromised, lost, stolen, accessed, and misused by unauthorized persons. Onix owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

93. Onix breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Onix's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of its patients' Private Information;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to HIPAA guidelines and industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

94. Onix negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

95. Had Onix remedied the deficiencies in its information storage and security systems

or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

The Data Breach Increases Victims' Risk Of Identity Theft

96. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

97. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[27]

98. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[28]

---

[26] 17 C.F.R. § 248.201 (2013).

[27] *Id.*

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Sept. 13, 2023).

99. For example, PII can be sold at a price ranging from $40 to $200.[29] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[30]

100. Theft of PHI is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[31]

101. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[32]

102. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your

---

[29] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Sept. 13, 2023).

[30] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Sept. 13, 2023).

[31] *What To Know About Medical Identity Theft,* Federal Trade Commission, (May 2021), *available at* https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last visited Aug. 3, 2023).

[32] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed Sept. 13, 2023).

> name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[33]

103. The Social Security Administration has further warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, apply for a job using a false identity, open bank accounts, and apply for other government documents such as driver's license and birth certificates.

104. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

105. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[33] Social Security Administration, Identity *Theft and Your Social Security Number*, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 13, 2023).

106. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[34]

107. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[35]

108. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, PHI, and Social Security numbers.

109. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

---

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Sept. 13, 2023).

[35] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Sept. 13, 2023).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[36]

110. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

111. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

112. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

113. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information

---

[36] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Sept. 13, 2023).

through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

114. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[37]

115. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

116. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

[37] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on Sept. 13, 2023).

117. The existence and prevalence of "Fullz" packages means that the Private Information stolen as a direct result of the Data Breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

118. Thus, even if certain information (such as driver's license numbers) was not stolen in the Data Breach, criminals can still easily create a comprehensive "Fullz" package.

119. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Plaintiffs & Class Members Suffered Harm as a Result of the Data Breach

120. Onix received Plaintiffs' PII/PHI in connection with providing certain services to them through one of Onix's affiliated groups. As discussed above, tin requesting and maintaining Plaintiffs' PII/PHI for business purposes, Onix expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' PII/PHI. Onix, however, did not take proper care of Plaintiffs' PII/PHI, leading to its exposure to and exfiltration by cybercriminals as a direct result of Onix's inadequate data security measures.

121. On or around May 26, 2023, Onix sent Plaintiffs a notice concerning the Data Breach. The letter stated that Onix experienced a cybersecurity attack and that the incident may have resulted in unauthorized access to Plaintiffs' PII/PHI stored on Onix's systems. The notice stated that the compromised information that was present on the impacted files included one or more of the following data elements: name, date of birth, patient number, social security number, financial account number, and/or health insurance information. Onix also offered identity theft protection services through Equifax, Experian and TransUnion, but only for a period of one year.

122. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited

to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

123. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. What's more, Defendant places the burden squarely on Plaintiffs and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

124. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

125. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.

126. For example, many victims of the Data Breach have suffered or will suffer ascertainable losses in the form of out- of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts;

f. Closely reviewing and monitoring Social Security number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come; and,

g. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

127. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[38]

128. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data

[38] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[39]

Diminution in Value of Private Information

129. PII and PHI are valuable property rights.[40] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

130. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[41]

131. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[42, 43]

---

[39] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Sept 13, 2023).

[40] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[41] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Sept 13, 2023).

[42] https://datacoup.com/ (last accessed Sept 13, 2023).

[43] https://digi.me/what-is-digime/ (last accessed Sept 13, 2023).

132. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[44]

133. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[45]

134. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

135. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

136. Moreover, because this information is immutable, *e.g.*, names, Social Security

---

[44] Nielsen Computer & Mobile Panel, *Frequently Asked Questions, available at* https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Sep. 13, 2023).

[45] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed Sep. 13, 2023).

numbers, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

137. Thus, Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

138. Defendant entirely failed to provide any compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Privat Information.

139. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Imminent and Continuing Risk of Future Fraud and Identity Theft

140. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

141. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

142. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

143. Defendant's delay in noticing affected persons of the theft of their Private Information prevented early mitigation efforts and compounded the harm.

144. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Personal and Medical Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Personal and Medical Information is not accessible online and that access to such data is password protected.

Lost Benefit of the Bargain

145. Plaintiffs greatly value their privacy, especially while receiving medical services and/or devices. Plaintiffs and Class Members did not receive the full benefit of their bargain when paying for and/or entrusting their inherently valuable Private Information to Defendant in exchange for medical services, instead receiving services that were of a diminished value to those described in their agreements with Onix.

146. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for and/or entrusted their valuable Private Information for (which would have included adequate data security protection) and the services they actually received.

147. Plaintiff and Class Members would not have obtained services from Onix had they known that Onix failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

PLAINTIFFS' EXPERIENCES

Plaintiff Eric Myers

148. Plaintiff Myers entrusted his Private Information to Defendant in order to receive medical care from one of Onix's affiliated medical groups.

149. Plaintiff Myers's Private Information was within the possession and control of Defendant at the time of the Data Breach.

150. Plaintiff Myers provided his Private Information to Defendant and trusted that the information would be safeguarded according to internal policies and state and federal law.

151. On or around May 26, 2023, Defendant notified Plaintiff Myers that Defendant's network had been accessed and Plaintiff's Private Information may have been involved in the Data Breach.

152. Plaintiff Myers is very careful about sharing his sensitive Private Information. Plaintiff Myers has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

153. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

154. As a result of the Data Breach, Defendant directed Plaintiff Myers to take certain steps to protect his Private Information and otherwise mitigate his damages.

155. As a result of the Data Breach, Plaintiff Myers spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred and set up a credit alert. This time has been lost forever and cannot be recaptured.

156. Moreover, this time was spent at Defendant's direction by way of the Data Breach notice where Defendant advised Plaintiff Myers to mitigate his damages by, among other things, monitoring his accounts for fraudulent activity.

157. Even with the best response, the harm caused to Plaintiff Myers cannot be undone.

158. Plaintiff Myers suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Myers entrusted to Defendant, which was compromised in and as a result of the Data Breach.

159. Plaintiff Myers suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

160. Defendant admits that Plaintiff Myers's Private Information was exfiltrated by criminal third-parties. Thus, Plaintiff Myers's and Class Members' information is already being misused by cybercriminals.

161. Plaintiff Myers has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

162. Plaintiff Myers has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Donald Owens

163. Plaintiff Owens provided his PII and PHI to one of Onix's affiliated medical groups as a condition of receiving treatment.

164. At the time of the Data Breach, Defendant retained Plaintiff Owens' PII/PHI in its system.

165. Plaintiff Owens is very careful about sharing his sensitive PII/PHI. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

166. Plaintiff was notified that his PII was compromised in the Data Breach.

167. Subsequent to the Data Breach, and in addition to the injuries above, Plaintiff Owens experienced actual fraud. In or around August 2023, an unauthorized individual tried to charge something from Apple in California to Plaintiff Owens' bank account. Plaintiff Owens had to travel to the bank to alert it that he was involved in a data breach. He additionally reached out to credit bureaus in an effort to mitigate his damages. Plaintiff Owens has also been receiving numerous emails about credit scores from Savvy, which is a site that is unfamiliar to him and for credit scores he did not request.

168. Plaintiff Owens estimates that he has spent an upward of 100 hours monitoring his accounts, traveling to the bank to discuss the fraudulent charges, changing his passwords on his accounts, resetting automatic billing instructions tied to compromised accounts, and otherwise addressing the Data Breach over the past several months. Plaintiff Owens plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his accounts for any unauthorized activity.

169. Plaintiff Owens suffers emotional stress from the public release of his PII/PHI and anxiety regarding the potential harm from this release.

Plaintiff Aida Albino Wimbush

170. Plaintiff Aida Albino-Wimbush provided her PII and PHI to one of Onix's affiliated medical groups as a condition of her employment at that facility.

171. At the time of the Data Breach, Defendant retained Plaintiff Wimbush's PII/PHI in

its system.

172. Plaintiff Wimbush is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

173. Plaintiff was notified that her PII was compromised in the Data Breach.

174. Subsequent to the Data Breach, and in addition to the injuries above, Plaintiff Wimbush experienced actual fraud. In or around July 27, 2023, an unauthorized individual made $780 in charges for Apple Care on Plaintiff Wimbush's account. Plaintiff Wimbush had to contact her bank to dispute the charges. Plaintiff Wimbush additionally took the proactive step of changing all of her passwords and had to resent billing instructions tied to the compromised bank account.

175. Plaintiff Wimbush further received a notification that her information had been found on the Dark Web.

176. Plaintiff Wimbush estimates that she has spent a total of approximately 120 hours monitoring her accounts, contacting her bank to discuss the fraudulent charges, changing her passwords on her accounts, resetting automatic billing instructions tied to compromised accounts, and otherwise addressing the Data Breach over the past several months. Plaintiff Wimbush plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

177. Plaintiff Wimbush suffers emotional stress from the public release of her PII/PHI and anxiety regarding the potential harm from this release.

Plaintiff Leah Simione

178. Plaintiff Simione provided her PII and PHI to one of Onix's affiliated medical groups as a condition of receiving treatment.

179. At the time of the Data Breach, Defendant retained Plaintiff Simione's PII/PHI in its system.

180. Plaintiff Simione is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

181. Plaintiff was notified that her PII was compromised in the Data Breach.

182. Subsequent to the Data Breach, and in addition to the injuries above, Plaintiff Simione has experienced an increase in spam calls. She also received a notification of a fraudulent attempt on her Amazon account to change her password in or around September 2023.

183. Plaintiff Simione estimates that she has spent approximately one hour monitoring her accounts for unauthorized activity and otherwise addressing the Data Breach. Plaintiff Simione plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

184. Plaintiff Simione suffers emotional stress from the public release of her PII/PHI and anxiety regarding the potential harm from this release.

Plaintiff Melissa Lyston

185. Plaintiff Melissa Lyston provided her PII and PHI to one of Onix's affiliated medical groups as a condition of receiving medical treatment.

186. At the time of the Data Breach, Defendant retained Plaintiff Lyston's PII/PHI in its system.

187. Plaintiff Lyston is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

188. Plaintiff was notified that her PII and PHI were compromised in the Data Breach.

189. Plaintiff Lyston received notification from Credit Karma that her information had been found on the Dark Web.

190. Starting several months ago, Plaintiff Lyston began receiving an excessive number of spam calls on the same cell phone number used at the Onix-affiliated medical group. These calls are a distraction, must be deleted, and waste time each day. Once the Notice Letter was delivered, and given the timing of the Data Breach, she believes that the calls are related to her stolen PII.

191. In addition, Plaintiff Lyston was recently denied credit but she is uncertain why. Since she is currently trying to buy a house, she is especially worried about the Data Breach's implications on her credit.

192. Plaintiff Lyston checks her accounts every day and estimates that she since the Data Breach, she has spent approximately 1-2 hours per day monitoring her accounts, getting a new debit card, and reviewing reports on Credit Karma. Plaintiff Lyston plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

193. Plaintiff Lyston suffers emotional stress from the public release of her PII/PHI and anxiety regarding the potential harm from this release.

Plaintiff Angela Haynie

194. Plaintiff Haynie provided her PII and PHI to one of Onix's affiliated medical groups as a condition of her employment with that facility.

195. At the time of the Data Breach, Defendant retained Plaintiff Haynie's PII/PHI in its system.

196. Plaintiff Haynie is very careful about sharing her sensitive PII/PHI. Plaintiff stores

any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

197. Plaintiff was notified that her PII was compromised in the Data Breach.

198. Subsequent to the Data Breach, and in addition to the injuries above, Plaintiff Haynie has been experiencing an increase in spam calls. She finds this suspicious as she is on the Do Not Call registry. Plaintiff Haynie additionally paid out-of-pocket for credit monitoring, which included a credit freeze, following the Data Breach. Plaintiff Haynie is also in the process of transferring her old accounts to new accounts as a result of the Data Breach in an attempt to mitigate the harm caused by the Data Breach.

199. Plaintiff Haynie estimates that she has spent an upward of 25 hours monitoring her accounts, transferring her accounts, resetting automatic billing instructions tied to compromised accounts, and otherwise addressing the Data Breach over the past several months. Plaintiff Haynie plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

200. Plaintiff Haynie suffers emotional stress from the public release of her PII/PHI and anxiety regarding the potential harm from this release.

Plaintiff Ashtyn Mark

201. Plaintiff Mark provided her PII and PHI to one of Onix's affiliated medical groups as a condition of receiving treatment.

202. At the time of the Data Breach, Defendant retained Plaintiff Mark's PII/PHI in its system.

203. Plaintiff Mark is very careful about sharing her sensitive PII/PHI. Plaintiff stores any documents containing his PII in a safe and secure location. She has never knowingly

transmitted unencrypted sensitive PII over the internet or any other unsecured source.

204. Plaintiff was notified that her PII was compromised in the Data Breach.

205. Subsequent to the Data Breach, and in addition to the injuries above, Plaintiff Mark has spent time reviewing her accounts daily in an attempt to help mitigate the damage caused by the Data Breach. Plaintiff Mark further received a notification that her information has been found on the Dark Web.

206. Plaintiff Mark estimates that she has spent approximately 15-20 hours monitoring her accounts for fraudulent activity and otherwise addressing the Data Breach over the past several months. Plaintiff Mark plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing her accounts for any unauthorized activity.

207. Plaintiff Mark suffers emotional stress from the public release of her PII/PHI and anxiety regarding the potential harm from this release.

CLASS ALLEGATIONS

208. Plaintiffs bring this action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure. Plaintiffs intend to seek certification of the Nationwide Class or, in the alternative, the Virginia, New Jersey and Pennsylvania Subclasses set forth below.

209. The **Nationwide Class** that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach (the "Nationwide Class" or "Class").

210. The **Pennsylvania Subclass** that Plaintiff Mark seeks to represent is defined as follows:

All individuals residing in the state of Pennsylvania whose Private Information was

compromised in the Data Breach (the "Pennsylvania Subclass").

211. The **Virginia Subclass** that Plaintiff Owens seeks to represent is defined as follows:

> All individuals residing in the state of Virginia whose Private Information was compromised in the Data Breach (the "Virginia Subclass").

212. The **New Jersey Subclass** that Plaintiffs Wimbush, Simione, and Lyston seek to represent is defined as follows:

> All individuals residing in the state of New Jersey whose Private Information was compromised in the Data Breach (the "New Jersey Subclass").

213. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

214. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

215. **Numerosity, Fed R. Civ. P. 23(a)(1)**: The Class is so numerous that joinder of all members is impracticable. According to the U.S. Department of Health and Human Services, the Data Breach compromised the information of 319,500 people.[46] The Class Members are identifiable within Defendant's records inasmuch as Defendant has already provided them with notification of the breach.

216. **Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3)**: Questions of law and fact are

[46] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Sept. 13, 2023).

common to the Class Members and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

b. Whether Defendant had duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or

nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

217. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of those of other Class Members because they all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

218. **Conduct Generally Applicable to the Class**: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

219. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

220. **Superiority and Manageability, Fed. R. Civ. P. 23(b)(3)**: The class litigation is

an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

221. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

222. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

223. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

224. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this complaint.

225. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

226. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and,

g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(*On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Pennsylvania, New Jersey and Virginia Subclasses*)

227. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

228. Onix collected the Private Information of Plaintiffs and Class Members in the ordinary course of providing services and/or employment to Plaintiffs and Class Members.

229. By collecting and storing this data in its computer system and network, and sharing it and using it for commercial gain, Onix owed a duty of care to use reasonable means to secure and safeguard its computer system—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Onix's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

230. Onix owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

231. Plaintiffs and the Class are a well-defined, foreseeable, and probable group of patients that Onix was aware, or should have been aware, could be injured by inadequate data security measures.

232. Onix owed numerous duties to Plaintiffs and the Class, including the following:

- To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- To protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

233. A large depository of highly valuable health care information is a foreseeable target for cybercriminals looking to steal and profit from that sensitive information. Onix knew or should have known that, given its repository of a host of Private Information for hundreds of thousands of patients posed a significant risk of being targeted for a data breach. Thus, Onix had a duty to reasonably safeguard its patients' data by implementing reasonable data security measures to protect against data breaches. The foreseeable harm to Plaintiffs and the Class of inadequate data security created a duty to act reasonably to safeguard the Private Information.

234. Onix's duty of care to use reasonable security measures also arose as a result of the special relationship that existed between Onix and patients. Onix was in a superior position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

235. Onix's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Onix is bound by industry standards to protect confidential Private Information.

236. Onix breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Onix includes, but is not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' Private Information;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

237. It was foreseeable that Onix's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

238. Onix's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing

to provide Plaintiffs and Class Members with timely notice that their sensitive Private Information had been compromised.

239. Neither Plaintiffs nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

240. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered damages as alleged above.

241. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

242. Plaintiffs and Class Members are also entitled to injunctive relief requiring Onix to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Pennsylvania, New Jersey and Virginia Subclasses)*

243. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

244. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Onix had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

245. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et seq.*, Onix also had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

246. Pursuant to HIPAA, Onix had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

247. Onix breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

248. Plaintiffs and Class Members were within the Class of Persons that HIPAA and the FTC Act are intended to protect and the harm resulting from the Data Breach is the type of injury against which the statutes are intended to guard.

249. Onix's failure to comply with applicable laws and regulations constitutes negligence per se.

250. But for Onix's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

251. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Onix's breach of its duties. Onix knew or should have known that it was failing to meet its duties, and that P Onix's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

252. As a direct and proximate result of Onix's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(*On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Pennsylvania, New Jersey and Virginia Subclasses*)

253. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

254. Plaintiffs and the Class Members entered into implied contracts with Onix under which Onix agreed to take reasonable measures to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class Members that their information had been breached and compromised.

255. Plaintiffs and the Class were required to and delivered their Private Information to Onix as part of the process of obtaining services provided by Onix Plaintiffs and Class Members paid money, or money was paid on their behalf, to Onix in exchange for services, or as a condition of their employment with a medical group affiliated with Onix.

256. Onix solicited, offered, and invited Class Members to provide their Private Information as part of Onix's regular business practices. Plaintiffs and Class Members accepted Onix's offers and provided their Private Information to Onix.

257. Onix accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services for Plaintiffs and Class Members.

258. In accepting such information and payment for services, Plaintiffs and the other Class Members entered into an implied contract with Onix whereby Onix became obligated to reasonably safeguard Plaintiffs' and the other Class Members' Private Information.

259. In delivering their Private Information to Onix and paying for healthcare services, Plaintiffs and Class Members intended and understood that Onix would adequately safeguard the data as part of that service.

260. Upon information and belief, in its written policies, Onix expressly and impliedly promised to Plaintiffs and Class Members that they would only disclose protected information and other Private Information under certain circumstances, none of which related to a Data Breach as occurred in this matter.

261. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under HIPAA or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

262. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

263. Plaintiffs and the Class Members would not have entrusted their Private Information to Onix in the absence of such an implied contract.

264. Had Onix disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and the other Class Members would not have provided their Private Information to Onix.

265. Onix recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

266. Plaintiffs and the other Class Members fully performed their obligations under the implied contracts with Onix.

267. Onix breached the implied contract with Plaintiffs and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

268. As a direct and proximate result of Onix's conduct, Plaintiffs and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV
BREACH OF FIDUCIARY DUTY
(*On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Pennsylvania, New Jersey and Virginia Subclasses*)

269. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

270. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

271. Defendant accepted and used Plaintiffs' and Class Members' Private Information for its own pecuniary benefit and accepted the Private Information with full knowledge of the need to maintain it as confidential, the need to implement appropriate data security measures, and the significant harm that would result to Plaintiffs and Class Members if the confidentiality of their Private Information was breached.

272. Defendant as their healthcare provider was in a superior position of trust and authority to Plaintiffs and Class Members.

273. Plaintiffs and Class Members had no way to ensure that Defendant's data security measures were adequate and no way to influence or verify the integrity of Defendant's data security posture.

274. Defendant knew that it was in an exclusive position to safeguard Plaintiffs' and Class Members' Private Information from the foreseeable threat of a ransomware attack and understood Plaintiffs' and Class Members' expectations that it safeguard their Private Information.

275. In light of the special relationship between Onix and Plaintiffs and Class Members, Onix became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Onix do store.

276. Onix had a fiduciary duty to act for the benefit of Plaintiffs and Class Members, in particular, to keep secure and confidential their Private Information.

277. Onix breached its fiduciary duty to Plaintiffs and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period.

278. Onix breached its fiduciary duty to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

279. Onix breached its fiduciary duty owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

280. Onix breached its fiduciary duty to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

281. As a direct and proximate result of Onix's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Onix's possession and is subject to further unauthorized disclosures so long as Onix fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Onix's services they received.

282. As a direct and proximate result of Onix's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(*On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, the Pennsylvania, New Jersey and Virginia Subclasses*)

283. Plaintiffs re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

284. This count is pleaded in the alternative to the above contract-based claims pursuant to Fed. R. Civ. P. 8.

285. Upon information and belief, Onix funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiffs and the Class Members.

286. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Onix.

287. Plaintiffs and Class Members conferred a monetary benefit on Onix. Specifically, they purchased goods and services from Onix and/or its agents and in so doing provided Onix with their Private Information. In exchange, Plaintiffs and Class Members should have received from Onix the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

288. Onix knew that Plaintiffs and Class Members conferred a benefit which Onix accepted. Onix profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

289. Plaintiffs and Class Members conferred a monetary benefit on Onix, by paying Onix as part of rendering medical services, a portion of which was to have been used for data security measures to secure Plaintiffs' and Class Members' Private Information, and by providing Onix with their valuable Personal Information.

290. Onix was enriched by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Onix instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by

utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Onix's failure to provide the requisite security.

291. Under the principles of equity and good conscience, Onix should not be permitted to retain the money and valuable Private Information belonging to Plaintiffs and Class Members, because Onix failed to implement appropriate data management and security measures that are mandated by industry standards.

292. Onix acquired the monetary benefit and Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

293. If Plaintiffs and Class Members knew that Onix had not secured their Private Information, they would not have agreed to provide their Private Information to Onix.

294. Plaintiffs and Class Members have no adequate remedy at law.

295. As a direct and proximate result of Onix's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Onix's possession and is subject to further unauthorized disclosures so long as Onix fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect,

contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

296. As a direct and proximate result of Onix's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

297. Onix should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them. In the alternative, Onix should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Onix's services.

COUNT VI
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. §§ 56:8-1, *et seq*. ("CFA")
(*On Behalf of Plaintiffs Wimbush, Simione, Lyston and the New Jersey Subclass*)

298. Plaintiffs Wimbush, Simione, and Lyston re-allege and incorporate by reference all preceding paragraphs as if fully set forth herein.

299. Plaintiffs Wimbush, Simione, and Lyston bring this Count on behalf of themselves and on behalf of the New Jersey Subclass (the "Class" for the purposes of this count).

300. The New Jersey Consumer Fraud Act ("CFA") makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J. Stat. Ann. § 56:8-2.

301. By the acts and conduct alleged herein, Defendant committed unfair acts and practices by:

a. failure to maintain adequate computer systems and data security practices to safeguard Private Information;

b. failure to disclose that its computer systems and data security practices were inadequate to safeguard Private Information from theft;

c. continued gathering and storage of Private Information and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach;

d. making and using false promises about the privacy and security of Private Information of Plaintiffs and Class Members, and;

e. continued gathering and storage of Private Information after Defendant knew or should have known of the Data Breach and before Defendant allegedly remediated the data security incident.

302. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act and the CFA.

303. The foregoing unfair acts and practices were directed at New Jersey consumers/purchasers.

304. Defendant, Plaintiffs, and Class Members are "persons" within the meaning of N.J. Stat. Ann. § 56:8-1(d).

305. Defendant engaged in "sales" of "merchandise" within the meaning of N.J. Stat. Ann. § 56:8-1(c), (d).

306. Defendant's unconscionable commercial practices set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiffs and members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of medical services from Defendant.

307. Plaintiffs and Class Members are New Jersey consumers who made payments or had payments made on their behalf to Defendant for the furnishing of medical services that were primarily for personal, family, or household purposes. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of medical services to consumers, including Plaintiffs and New Jersey Subclass Members.

308. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and providing administrative services to consumers in the State of New Jersey.

309. As a direct and proximate result of Defendant's unlawful conduct, Plaintiffs and Class Members have suffered an ascertainable loss, damages, and are at present risk of further harm.

310. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's unlawful conduct.

311. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

312. On behalf of themselves and other members of the New Jersey Subclass, Plaintiffs are entitled to recover legal and/or equitable relief, including an order enjoining Defendant's unlawful conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. Stat. Ann. § 56:8-19, and any other just and appropriate relief.

COUNT VII
VIOLATION OF PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW ("CPL")
(On Behalf of Plaintiff Mark and the Pennsylvania Subclass)

313. Plaintiff Mark re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

314. Plaintiff Mark brings this Count on behalf of herself and on behalf of the Pennsylvania Subclass (the "Class" for the purposes of this count).

315. Pennsylvania's Unfair Trade Practices and Consumer Protection Law prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." 73 Pa. Stat. Ann. § 201-3.

316. Plaintiff and Class members are consumers as defined by the statute.

317. Defendant engaged in unfair acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of the CPL, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII and PHI, which was a proximate and direct cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents involving other organizations, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII and PHI, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII and PHI; and

f. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45.

318. Defendant's unfair acts were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of PII and PHI.

319. Defendant acted intentionally and knowingly to violate the CPL, and recklessly disregarded Plaintiff's and Class Members' rights.

320. As a direct and proximate result of Defendant's unfair and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII and PHI; and the other harms detailed herein.

321. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

322. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff and Class members that they could not reasonably avoid.

COUNT VIII
VIRGINIA CONSUMER PROTECTION ACT,
Va. Code Ann. §§ 59.1-196, et seq.
(On Behalf of Plaintiff Owens and the Virginia Subclass)

323. Plaintiff Owens re-alleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

324. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

325. Defendant is a "person" as defined by Va. Code Ann. § 59.1-198.

326. Defendant is a "supplier," as defined by Va. Code Ann. § 59.1-198.

327. Defendant engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Defendant advertised, offered, or sold goods or services used primarily for personal, family or household purposes.

328. Defendant engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

329. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

330. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Class Members, about the adequacy of Defendant's computer and data security and the quality of the Defendant brand.

331. Had Defendant disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in

business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant was trusted with sensitive and valuable PII of its patients, including Plaintiffs and the Class. Defendant accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and the Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

332. In Defendant had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the PII in its possession, and the generally accepted professional standards. Such a duty is implied by law due to the nature of the relationship between consumers including Plaintiffs and the Class – and Defendant, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Defendant. Defendant's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Class that contradicted these representations.

333. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain characteristics, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised;

d. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

334. Defendant acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiffs and Class Members' rights. Defendant's numerous past data breaches put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Defendant for its wrongdoing and warn or deter others from engaging in similar conduct.

335. As a direct and proximate result of Defendant's deceptive acts or practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Breach.

336. Defendant's violations present a continuing risk to Plaintiffs and Class Members as well as to the general public.

337. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the

conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully pray for judgment in their favor and against Onix as follows:

A. For an Order certifying the Nationwide Class and state subclasses and appointing Plaintiffs and their Counsel to represent such Classes;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for

threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, statutory, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: September 15, 2023

Respectfully Submitted,

/s/ _____

Benjamin F. Johns (PA Bar 201373)
Samantha E. Holbrook (PA Bar 311829)
Andrea L. Bonner (PA Bar 332945)
SHUB & JOHNS LLC

Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
Telephone: (610) 477-8380
Fax: (856) 210-9088
bjohnes@shublawyers.com
sholbrook@shublawyers.com
abonner@shublawyers.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Co-Lead Counsel for Plaintiffs

Bryan L. Bleichner*
Phillip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Ave., Ste 1700
Telephone: 612-767-3602
Fax: 612-336-2940
bbleicherner@chestnutcambronne.com
pkrzeski@chestnutcambrone.com

Nicholas Sandercock
SIRI & GLIMSTAD LLP
745 5th Avenue, Suite 500
New York, NY 10151
Tel: (212) 532-1091
nsandercock@sirillp.com

Gary E. Mason*
Danielle Perry*
Lisa A. White*
MASON LLP
5335 Wisconsin Avenue, NW
Suite 640
Washington, DC 20015
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

James M. Evangelista*
EVANGELISTA WORLEY LLC
500 Sugar Mill Road Suite 245A
Atlanta, GA 30350
Tel.: 404-205-8400
Fax: 404-205-8395
Email: jim@ewlawllc.com

Jennifer Czeisler*
JKC LAW, LLC
269 Altessa Blvd. Melville, NY 11747
Tel: (516)457-9571
Email: jennifer@jkclawllc.com

James A. Francis
John Soumilas
Lauren KW Brennan
Jordan M. Sartell*
FRANCIS MAILMAN SOUMILAS, P.C.
1600 Market Street, Suite 2510
Philadelphia, PA 19103
T: (215) 735-8600
F: (215) 940-8000
jfrancis@consumerlawfirm.com
jsoumilas@consumerlawfirm.com
lbrennan@consumerlawfirm.com
jsartell@consumerlawfirm.com

David S. Almeida*
Elena A. Belov*
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
Tel: (312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Attorneys for Plaintiffs and the Proposed Class

**pro hac vice*

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 15th day of September 2023, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the e-mail addresses denoted on the Electronic Mail notice list.

/s/ Benjamin F. Johns
Benjamin F. Johns